Práctica: SSO contra Directorio Activo

Objetivo: Modificar el sistema a autenticación para montar un sistema SSO

Desarrollo:

1. Utilizar dcpromo para elevar la máquina virtual a un controlador de dominio, con nombre ATOS.COM
2. Descomprimer el componente security-negotiation-2.0.3.SP02 y copiar el Jar jboss-negotiation.jar a la carpeta C:\jboss-5.1.0.GA\common\lib
3. Modificar el fichero war-deployers-jboss-beans.xml de la carpeta C:\jboss-5.1.0.GA\server\default\deployers\jbossweb.deployer\META-INF para colocar un nuevo sistema de autenticación a través del navegador

```
<entry>
  <key>SPNEGO</key>
  <value>org.jboss.security.negotiation.NegotiationAuthenticator</value>
</entry>
```

4. Añade al fichero properties-service.xml la siguiente propiedad, para indicar donde se encuentra el servidor de distribución de claves y el ámbito donde aplica:

```
<attribute name="Properties">
   java.security.krb5.kdc=demosjava.atos.com
   java.security.krb5.realm=ATOS.COM
</attribute>
```

5. Crear una cuenta de dominio: jbosslogin donde se encuentren configuradas estas propiedades:
   5.1. El usuario no puede cambiar la password
   5.2. La contraseña nunca caduca
   5.3. No se requiere preautenticacion kerberos

6. Instala las herramientas de soporte de Windows 2003
7. Mapea la cuenta de usuario del directorio activo jbosslogin a una cuenta del host que será utilizada por Jboss

```
setspn.exe -a HTTP/demosjava.atos.com@ATOS.COM jbosslogin
```

8. Comprueba el mapeo

```
setspn.exe -l jbosslogin
```

9. Volcamos el usuario y el mapeo a un fichero de confianza para ser utilizado en el servidor de app

```
ktpass -princ HTTP/demosjava.atos.com@ATOS.COM -pass * -mapuser ATOS\jbosslogin /ptype
KRB5_NT_PRINCIPAL–out
c:\jbosslogin.http.keytab
```

10. Por último se exporta la tabla la tabla que va a ser utilizada por el servidor Java

```
ktab -k c:\jbosslogin.http.keytab -a jbosslogin@ATOS.COM
```

11.
12. Creamos una política en el fichero login-config.xml para acceder al servidor de claves

```
<application-policy name="host">
  <authentication>
    <login-module code="com.sun.security.auth.module.Krb5LoginModule" flag="required">
      <module-option name="storeKey">true</module-option>
      <module-option name="useKeyTab">true</module-option>
      <module-option name="principal">HTTP/demosjava.atos.com@ATOS.COM</module-option>
      <module-option name="keyTab">/usr/local/jbosslogin.http.keytab</module-option>
```

```
        <module-option name="doNotPrompt">true</module-option>
        <module-option name="debug">true</module-option>
      </login-module>
    </authentication>
</application-policy>
```

13. Creamos dos ficheros para almacenar usuario y roles, el de usuarios lo dejamos vacios pues estos se van a autenticar con el AD:
    13.1. props/spnego-users.properties
    13.2. props/spnego-roles.properties
14. sfd
15. Mientras que el fichero de usuarios lo dejamos en blanco el de roles lo rellenamos con el mapeo de usuarios y roles

```
administrador@ATOS.COM=Usuario
```

16. Creamos la política JAAS en el fichero login.config.xml

```
<application-policy name="SPNEGO">
  <authentication>
    <login-module
      code="org.jboss.security.negotiation.spnego.SPNEGOLoginModule"
      flag="requisite">
      <module-option name="password-stacking">useFirstPass</module-option>
      <module-option name="serverSecurityDomain">host</module-option>
    </login-module>
    <login-module code="org.jboss.security.auth.spi.UsersRolesLoginModule" flag="required">
      <module-option name="password-stacking">useFirstPass</module-option>
      <module-option name="usersProperties">props/spnego-users.properties</module-option>
      <module-option name="rolesProperties">props/spnego-roles.properties</module-option>
    </login-module>
  </authentication>
</application-policy>
```

17.
18. Modificamos el fichero jboss-web.xml de la aplicación para que utilice como política JAAS SPNEGO y modificamos el fichero web.xml para que utilice SPNEGO como sistema de autenticación